Specification-Based Intrusion Detection for Mobile Ad Hoc Networks

Elisabeth Hansson
Swedish Defence Research Agency
Dept. of System Development and IT Security
Box 1165
58111 Linköping
SWEDEN

E-mail: Elisabeth.Hansson@foi.se

ABSTRACT

New challenges within the area of security have arisen due to a relatively new paradigm called mobile ad hoc networks. A mobile ad hoc network consists of wireless nodes that build a radio network without any pre-existing infrastructure or centralized servers. However, these networks have inherent vulnerabilities that make them susceptible to malicious attacks such as denial of service, propagation of incorrect routing information, and physical compromise of nodes. Current security solutions for tactical radio networks, which mainly are based on cryptography, are not sufficient. A new solution for intrusion detection is needed to obtain an acceptable level of security. In this paper, we make two contributions to the area of secure mobile ad hoc networks. First, we present an entirely new architecture for intrusion detection applicable to mobile ad hoc networks. Second, we also present a specification-based approach that detects attacks against mobile ad hoc networks.

1.0 INTRODUCTION

In recent years, with the rapid development and increased usage of wireless devices, security has become one of the major problems that wireless networks face. A mobile ad hoc network is a wireless network that can be rapidly deployed as a multihop radio network without using any centralized functionality or fixed infrastructure such as base stations. Applications of mobile ad hoc networks include the tactical communication in a battlefield, rescue missions, as well as civilian ad hoc situations like conferences.

Securing mobile ad hoc networks is a challenge. A mobile ad hoc network has inherent vulnerabilities that make it susceptible to malicious attacks such as denial of service attacks, message replay, propagation of incorrect routing information, and physical compromise of nodes (see more on this in the following section). Therefore, the traditional way to protect radio networks by cryptographic mechanisms, such as encryption and authentication, is no longer sufficient. Cryptography can reduce the amount of successful intrusions, but cannot fully eliminate them. Encryption and authentication provide protection against some attacks from external nodes, but will not protect against attacks from inside nodes, which already have the required keys [1][2]. Furthermore, it is difficult to design and implement software systems without introducing design and programming errors that an adversary can exploit. If an adversary has adequate resources and tries hard enough, there is a risk that the adversary succeeds in infiltrating the system.

Hence, to obtain an acceptable level of security in military contexts, traditional security solutions should be coupled with *intrusion detection systems* (IDS) that continuously monitor the network and determine whether the system (the network or any node of the network) is under attack. Once an intrusion is

Hansson, E. (2006) Specification-Based Intrusion Detection for Mobile Ad Hoc Networks. In *Military Communications* (pp. P3-1 – P3-14). Meeting Proceedings RTO-MP-IST-054, Poster 3. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Specification-Based Intrusion Detection for Mobile Ad Hoc Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Swedish Defence Research Agency Dept. of System Development and IT Security Box 1165 58111 Linköping SWEDEN**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202750. RTO-MP-IST-054, Military Communications (Les communications militaires), The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**14**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

detected, e.g. in the early stage of a denial of service attack, a response can be put into place to minimize the damage.

Intrusion detection can be classified into three broad categories [14]: anomaly detection, misuse (signature) detection, and specification-based detection. *Anomaly detection* recognizes deviations from normalcy by building models of normal behaviour. Any deviation from normal is identified as an attack. *Misuse detection* use patterns of known attacks to recognize intrusions. *Specification-based detection* detects attacks with use of a set of constraints (rules) that define the correct operation of a program or a protocol.

So far, there are no commercial intrusion detection systems that are applicable to mobile ad hoc networks [16]. However, a few researchers have proposed methods for intrusion detection applicable to mobile ad hoc networks. The state of the art of intrusion detection for wireless ad hoc networks is described by Mishra et al [8]. Zhang and Lee have described a distributed and cooperative intrusion detection method where every node in the network participates in intrusion and response [5]. The problem with their architecture is that it relies on cooperative participation between nodes for detection and response, even though the purpose really is to determine if any of these nodes are malicious. Furthermore, Zhang, Lee and Huang have proposed a method to detect attacks against protocols based on anomalies [2]. The result of their experiments showed that anomalies may be used for detecting routing attacks, but the methods really need to be refined. Their method resulted in many false alarms. Moreover, Sergio Marti et al. have proposed a watchdog technique that intended to detect malicious neighbour nodes by listening on their incoming and outgoing traffic [15]. Their method resulted in a lot of problems that still are unsolved.

In this paper, we make two contributions to the area of secure mobile ad hoc networks. First, we propose a new architecture for intrusion detection, based on specification-based detection, which is applicable to a mobile ad hoc network. Second, we present a specification-based approach that detects attacks in protocols based on a set of constraints that describe the correct operations of the protocols.

It is assumed that military mobile ad hoc networks are equipped with strong encryption at the data link layer or network layer. The purpose of the proposed intrusion detection method is to complement the encryption solution in order to provide a higher level of security.

Intrusion detection should be distributed to suit the architecture and features of a mobile ad hoc network [5]. We propose an architecture where every node is responsible for detecting intrusions locally in the node by listening on the receiving and transmitting interface of the node. A difference, compared with other proposed methods for mobile ad hoc networks, is that the intrusion detection technique is specification-based. Furthermore, whereas other proposed solutions mainly aim at identifying misbehaving neighbour nodes and perform responses against them, the proposed solution aims at detecting intrusions within the node. Thus, the intrusion detection system will determine if the node itself is misbehaving and also internally respond to detected intrusions. Our intrusion detection system resides in the network card in a tamper-resistant processor.

To illustrate our approach, we present a specification-based method that detects attacks against the standardized Ad hoc On-demand Distance Vector (AODV) routing protocol [13]. This is achieved by modelling the AODV protocol with the extended finite state machine method [18]. It is suitable to illustrate the approach for routing protocols, since these protocols implement typical characteristics of mobile ad hoc networks and also are vulnerable to an adversary's malicious attacks. However, we believe that the principle behind the approach also is applicable to other protocols as well even though the protocols may differ in the format.

The structure of the paper is as follows. In section 2, we describe security vulnerabilities of mobile ad hoc networks. Next, a new architecture for intrusion detection is described in section 3. In section 4, the specification-based approach is illustrated for AODV. Conclusions are described in section 5.

2.0 SECURITY VULNERABILITIES

Some of the critical requirements that mobile ad hoc networks are designed to meet, such as flexibility and robustness, naturally come at the cost of higher security challenges. In addition to the security threats common in fixed networks, some characteristics of mobile ad hoc networks impose further vulnerabilities. A tactical mobile ad hoc network is vulnerable to attacks because of its poor physical protection, wireless links, dynamic network topology, the property that each node is a router, the property of self-configuration, distributed algorithms and lack of clear line of defence. These vulnerabilities are described in section 2.1. AODV routing protocol vulnerabilities are described in section 2.2.

2.1 Vulnerabilities in mobile ad hoc networks

Medium access is simple in wireless mobile ad hoc networks. The wireless link allows passive eavesdropping but also simplifies active impersonation, message replay and message distortion [8]. Eavesdropping might give the adversary access to secret confidential information. Active attacks might results in, e.g., impersonation of a node or disruption of the communication in the network.

Mobile nodes in a hostile environment have poor physical protection [4]. A mobile node can be stolen or hijacked or an intruder can penetrate the security mechanisms and perform attacks from the node by injecting, e.g., a Trojan. The possibility of compromised malicious nodes performing internal attacks is probably one of the most severe threats to a mobile ad hoc network. Thus, we must not only consider attacks from external nodes, but also take into account attacks from internal compromised nodes.

To achieve an autonomous ad hoc network many protocols developed for mobile ad hoc network are based on distributed algorithms. These distributed algorithms enable new types of attacks, since the algorithms are based on the cooperative participation of nodes. If one node is malicious it can affect the entire network. For example, although there are many MAC protocols, their basic working principles are similar. In a contention-based MAC protocol nodes must follow rules to reduce or avoid collisions. A malicious node not obeying the rules can create unfairness and congestion in the network. In a contention-free MAC protocol, each node must obtain an agreement from all other nodes to use the channel resource. In both cases, a malicious node not cooperating can create disruption of the network [9][10].

IP address auto configuration introduces vulnerabilities. For example, the IPv6 stateless address auto configuration [12] and the similar auto configuration principle above IPv4 are vulnerable to false replies by malicious nodes. Both methods rely on the verification that a particular address is not already used by performing Duplicate Address Detection (DAD) [11]. A malicious node can pretend to use any of the address chosen by the incoming node, thus denying it the right to join the network.

Moreover, the fact that each node is a router also causes threats to all nodes. To reach the destination, the route from a node takes the packets across the network through various unknown nodes. Thus, an intermediate node can perform arbitrary man-in-the-middle attacks such as eavesdrop, modify and drop packets.

An additional threat, related to each node being a router, is attacks against the distributed routing protocols developed for mobile ad hoc networks. Routing attacks can be classified in routing disruption attacks and resource consumption attacks [3]. In routing disruption attacks packets are routed improperly whereas resource consumption aims at using up resources such as bandwidth, memory and computation capacity.

Finally, compared to a wired network, the mobile ad hoc network is vulnerable to several external attacks, since there is no clear line of defence such as a firewall. In wired networks, attacks against a node normally have to pass at least one centralized security mechanism, e.g. a firewall, whereas attacks against a mobile ad hoc network target the node directly. For example, the centralized firewall in wired networks can protect against several data link layer attacks.

2.2 AODV vulnerabilities

AODV is a standardized routing protocol designed for mobile ad hoc networks [13]. The algorithm is on-demand. That is, builds routes between nodes, when the source node needs them. AODV uses three routing packets to build a route to a destination: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). When a node does not have a route to a destination, which it want to communicate with, it broadcasts a Route Request in which it ask for a route to the destination.

When a node receives a Route Request, it sends a Route Reply, if the node is the destination node. An intermediate node can also respond to the request, if it has a fresh route to the specified destination in its route table. A route is considered fresh if the sequence number in the Route Request is lower than the corresponding value in the routing table or the sequence numbers are equal but the hop count is smaller.

The route is maintained as long as the route remains active. A route is considered active if data are sent from the source node to the destination node. If a link break occurs in an active route, a Route Error is propagated to the source node. Vulnerabilities of AODV are described in Table 1 below.

Table 1: AODV vulnerabilities

Type of attack	Attack description	Misuse goal
False Message Propagation of RREQs	1. An adversary impersonates a node and sends RREQs with the originator IP address of the other node in order to create route disruption. An adversary may also falsify other fields of the RREQ, e.g., false hop count in order to create false network picture.	Route disruption. For example, redirect traffic or disrupt communication.
False Message Propagation of RREPs	2. The node sends a forged RREP with an existing false originator IP address even though the node have not received any related RREQ.	Route disruption.
False route reply	3. These attacks are carried out by falsified reply to a valid RREQ. A malicious node advertises a route in the RREP to a node with a false destination sequence number (e.g. greater than the authentic value) or falsified value of the hop count.	Route disruption or suboptimal tour.
Rushing	4. To limit the overhead, each node typically forwards only one RREQ originating from any Route Discovery (identified by RREQ identity). In the rushing attack, an adversary sends RREQs with a false originator IP address and guessed value of the RREQ identity in order to suppress later transmitted legitimate RREQs from the impersonated node [3].	The misuse goal of the attack is to prevent a new route from being established.
Modification of routing messages	5. A malicious node modifies a field in a received RREP (or RREQ) and then forwards it to its neighbours.	Route disruption.
Resource depletion attack	6. Resource depletion refers to consuming the communication bandwidth in the network, computer capacity or storage space at individual nodes. This can be achieved by flooding the network with RREQs or RREPs.	Resource consumption.
Dropping of routing packets	7. The attacker simply drops (all or some) received routing messages.	No consequence, suboptimal tour or divided network.
Routing table overflow	8. A malicious node floods the network with non-existing routes by sending RREQs with non-existing originator addresses or RREPs with non-existing destination addresses.	Route disruption.
Modify routing table	9. An adversary modifies the routing table.	Route disruption.
Maintenance attack	10. A malicious node propagates false RERR messages.	Route disruption.

3.0 AN ARCHITECTURE FOR INTRUSION DETECTION

In this section a new architecture for intrusion detection is proposed. Intrusion detection in mobile ad hoc networks should be distributed to suit the architecture and features of a mobile ad hoc network [5]. We propose an architecture where every node is responsible for detecting local intrusions by listening on the receiving and transmitting interface of the node. Thus, all nodes contain an intrusion detection system (IDS) agent. The IDS agent will detect if the node performs attacks against other nodes by using specification-based detection.

3.1 The IDS agent

Even though the IDS agent is fairly complex it can be structured in five modules, see figure 1.

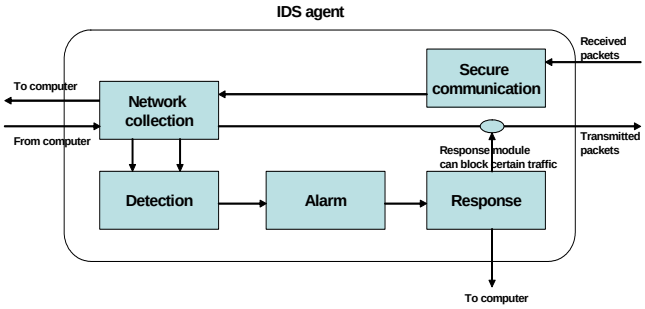

Figure 1: IDS agent

Network collection module

The network collection module gathers packets received from neighbour nodes and forwards the selected packets to the detection module. Likewise, packets transmitted from the node to other nodes are gathered and forwarded to the detection module.

Detection module

The purpose of the proposed intrusion detection system is to detect intrusions against protocols developed for mobile ad hoc networks. So far, these protocols reside in the network layer. Thus, the detection module processes local data received from the network collection module to detect intrusions via the network layer.

The ability to detect previously unknown attacks is essential in military contexts, since some military organizations have resources to develop attacks that are unknown and not used in civilian contexts. Thus, the aim is to provide a method that detects previously unknown attacks. So far, the only method proposed for mobile ad hoc networks to detect previously unknown attacks is by anomaly detection. The techniques proposed by Zhang et al result in too many false alarms [2]. However, specification-based detection has been suggested for wired networks. Experiments in wired networks show that specification-based detection may provide the capability to detect previously unknown attacks, while providing a low false positive rate, i.e., few false alarms [6][7]. Thus, our detection module detects attacks with specification-based detection. The approach is illustrated for AODV in section 4.

Alerting module

The alerting module takes input from the internal detection module. The information of intrusions from the detection module is processed to categorize the attacks according to their consequence and also minimize the number of false alarms.

For example, the detection module can with high accuracy determine if the node has neglected to forward a routing packet, but this is not necessarily an attack. This could be explained by, e.g., a full buffer. The consequence of one dropped routing packet is limited. Thus, there is no reason to take actions against it. However, if all routing packets are dropped within a certain time period it probably would affect the overall performance. This should be reported as misbehaving to the respond module whether it depends on an intrusion or not.

Response module

A malicious node should not be able to produce malicious responses against other nodes. At the same time, typical features of an ad hoc network are distributed functionality and a high degree of automatization. To consider these features any node must be able to act against detected intrusions without human intervention and without collaboration with other nodes. This is accomplished by *internal responses*. Below are some examples of responses;

- The IDS agent can demand the user of the node to re-authenticate to reduce the risk that the node is stolen and used for malicious purposes. Note that all responses are internally performed. Thus, the IDS agent can only request the user of its own node to re-authenticate.
- If the detected attack has minor consequences the user is recommended to perform maintenance of the node, when it is possible.
- If the detected attack has serious consequences, such as injecting malicious routing packets that disrupt the entire communication in the network, the outgoing routing packets from the node are blocked.

Secure communication

The main task of the secure communication module is to verify that packets received from other nodes have been processed with the correct version of the IDS agent. This is similar to the commonly used HTTPS, which secure web traffic. An HTTPS server or client can be configured to only communicate with a party that uses a certain version of the protocol, e.g. SSL[1] version 3.0.

The IDS agent forwards hash chains with its neighbours, after having done an initial signature [19].

3.2 IDS agent in the network card

The purpose of the IDS agent is to determine if the node itself is misbehaving, i.e., performing internal attacks against other nodes. An internal attack can come from an unauthorized user, which has stolen or hijacked the node, and uses it for malicious purposes. It is also possible that an authorized user (bribed, deceived or dissatisfied) performs internal attacks. Furthermore, attacks can also come from adversaries without having physical access to the node. For example, it is common practice to send e-mail with an attachment that contains malicious software. The malicious software could propagate from the node via the network to other nodes. Moreover, attacks can also come from someone that has succeeded to take over the node by exploiting software errors. To conclude, the IDS agent should protect against internal attacks that originates from users that have or not have physical access to the node.

Unauthorized access from the malicious software or malicious user is considerably delayed by putting the IDS agent in a tamper-resistant processor on the network card. A tamper-resistant processor includes hardware and software to deny (or at least delay) unauthorized access by using cryptographic means.

Furthermore, it is natural to put the IDS agent on the network card, since the IDS makes conclusions about intrusions on collected network traffic. Another reason for putting the IDS agent on the network card is that the IDS also may block certain traffic. For example, the response against a routing attack with serious consequence is to block outgoing routing traffic. The IDS agent must also block traffic from nodes that are not equipped with the correct version of the IDS agent, see section 3.1 secure communication.

To accomplish industrialization of the IDS, “plug-and-play” should be possible. For example, the solution should not require changes in the software of the computer (e.g. the operating system). Thus, the outgoing and ingoing interfaces of the network card are not changed, i.e., the network circuits remain the same.

[1] SSL stands for Secure Socket layer. SSL can be used with HTTP to perform authentication and encyption of web traffic.

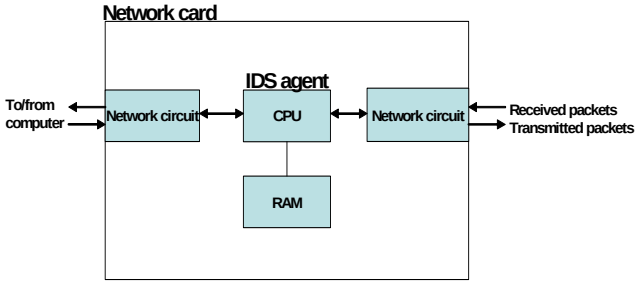

Figure 2: Network card with IDS agent

3.3 Pros and cons of internal intrusion detection and response

The IDS agent responds to detected attacks with internal responses. The advantage with internally performed response is that an adversary can not use the intrusion detection system to produce responses against other nodes. Nevertheless, the methods of internally performed response are just as effective as global responses and also easier to perform. For example, other researchers have proposed to exclude an identified compromised node that performs attacks against other nodes with forced re-keying [2][8]. This is a complex solution. First, a method is needed to decide which node or nodes are trusted to exclude another node from the network. It is difficult to know which the trusted nodes are. Second, forced re-keying must be performed in a secure way with a distributed key method. Our solution with internal response, e.g., block outgoing malicious traffic, is far simpler and also effective.

Another advantage with the proposed solution is that it does not require any cooperation with other nodes. This is advantageous, since it is difficult to know which the trusted nodes are.

Another advantage with the proposed solution is that it automatically performs responses without any human intervention.

However, the IDS agent should be protected from unauthorized access, since the IDS is supposed to detect internal attacks. An internal attack can come from an adversary with or without physical access. To considerably delay access the IDS agent is put in a tamper-resistant processor. The tamper-resistant processor will prevent adversaries, which do not have physical access, from modifying the IDS agent. Current techniques for tamper-resistant processor can also considerably delay an adversary with physical access from modifying the IDS agent. It is enough to considerably delay access, since the node is assumed to be provided with strong encryption at the data link layer or network layer. Today, the keys for data link layer (or network layer) encryption are manually exchanged at least every day. There is no indication that this will be performed differently in the near future. Thus, it is enough to delay the access for one day. However, it can never be proven that any security solution really is totally secure. Thus, the aim of the IDS agent is to increase the security of the node and make it more difficult to perform successful attacks.

4.0 SPECIFICATION-BASED DETECTION IN MOBILE AD HOC NETWORKS

Specification-based detection defines a set of rules that describe the correct operation of a protocol and monitors the execution of the protocol with respect to the defined rules. In other words, the specification-based approach provides a model of the protocol in order to detect attacks based on protocol specification. The specifications are usually derived manually from RFCs or other descriptions of protocols. However, a challenge in specification-based detection is how to define the set of rules that describe the correct operation of the protocols to efficiently detect attacks. In this paper, this is achieved by modelling the protocol with the extended finite state machine method.

4.1 Extended finite state machine (EFSM)

A finite state machine is a model of computation consisting of a set of states, a start state, an input alphabet, and a transition function that maps input symbols and current states to a next state [17]. The behaviour of the finite state machine can be described graphically in the form of a state transition diagram, as shown in figure 3a. That is, the state transition diagram specifies a set of transition functions for each state of the machine. These transition functions combined with input strings determine the next state of the finite state machine for a given state. If no transition rule is executable, the machine is said to be in an end-state.

However, the finite state machine computation model is insufficient to model the AODV protocol, since it lacks the ability to model the transfer of arbitrary values and manipulate variables conveniently. Therefore, AODV is modeled using the extended finite state machine, which is an extended version of the finite state machine with two major differences [18]. First, the extended finite state machine uses variables that have symbolic names and hold abstract objects, which in this case are integer values. Second, logical operators are used to manipulate the contents of the variables, as shown in figure 3b.

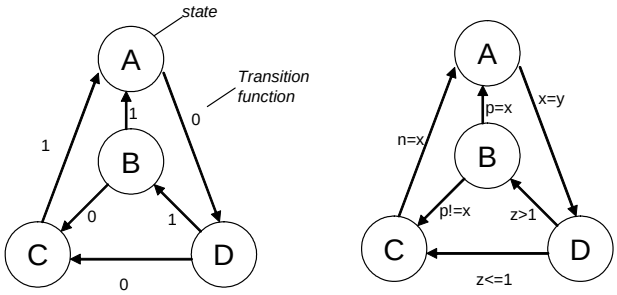

Figure 3: FSM State Transition Diagram (a) and EFSM State Transition Diagram (b)

4.2 AODV specification

The proposed AODV specification is an abstract of the AODV protocol specified in RFC 3561 [13]. That is, only essential details of the protocol are modelled in order to detect if the node performs attacks against other nodes. First, the network collection module of the IDS agent gathers routing packets received from neighbour nodes and routing packets sent to other nodes. Next, the AODV state machine examines the transmitted routing packets from the node to detect if the node is performing routing attacks against other nodes. This is achieved by creating an instance of the AODV state machine for each transmitted routing packet to a certain destination. If an instance of the AODV state machine already exists for the destination, the instance is updated with information from the transmitted routing message.

AODV is modelled in two transition diagrams; Route Request and Route Reply. In the future, also RERR messages will be modelled. For each RREQ transmitted to a unique destination, we create an instance of the AODV state machine that starts in the *RREQ transmitted* state, see figure 4. Similarly, we also create instances of the AODV state machine for every transmitted RREP to a certain destination. Thus, there can be many instances of the state machine in runtime. It is important to find a way to limit the number of instances of the AODV state machine to save memory and computer capacity. Therefore, an instance of the AODV machine for a certain destination is deleted automatically when the state machine instance reach the final state (end-state). Thus, the maximal number of state machines is equal to the number of nodes in the network multiplied by two.

The RREQ transition diagram is depicted in figure 4 whereas the RREP transition diagram is depicted in figure 5. It is described in section 4.3 how these specifications can detect intrusions.

State machines of protocols often have more than one transition rule per state, i.e. a non-deterministic choice. In our proposal, there are several transition rules for some states, but they are mutually exclusive. That is, at any time only one, or none, of the transitions is valid. Thus, a given input signal to a certain state always results in only one state.

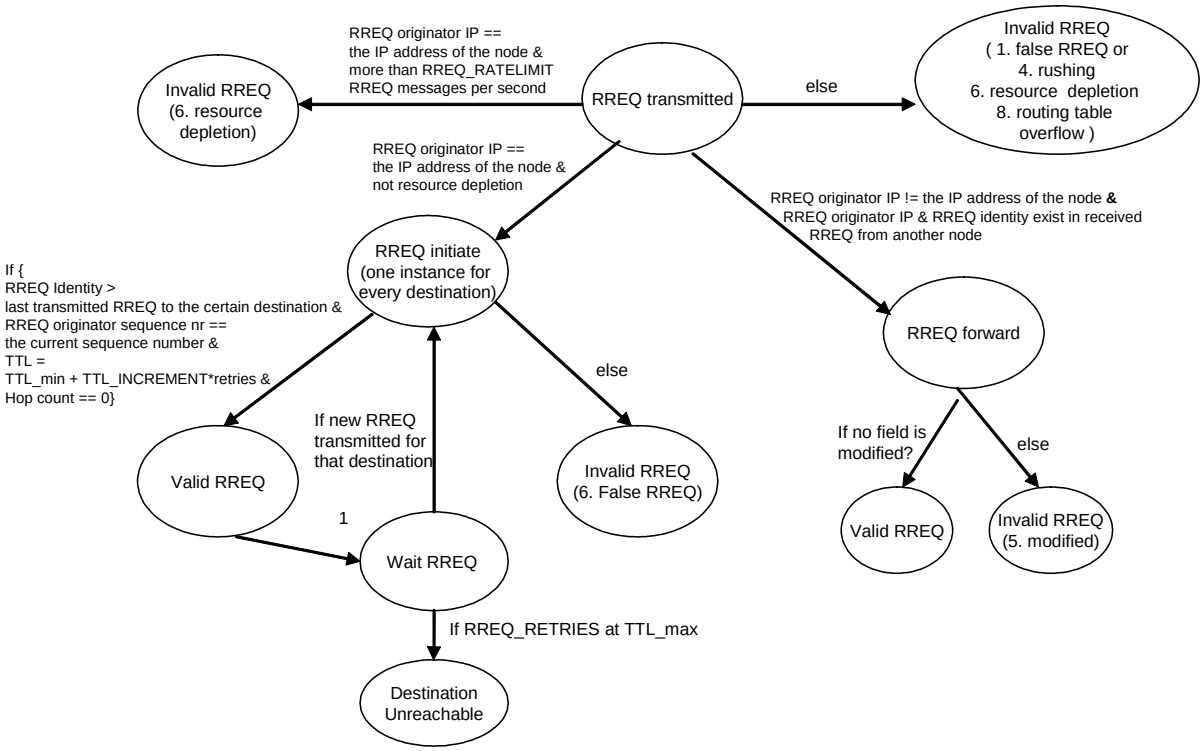

Figure 4: AODV RREQ transition diagram

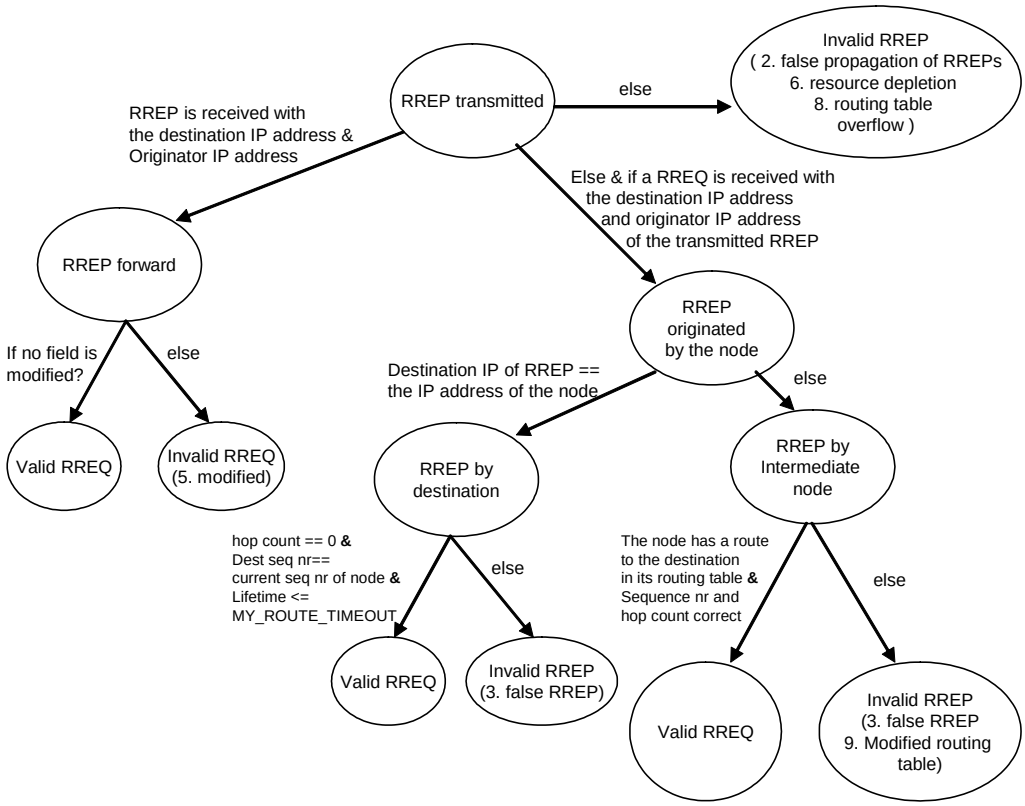

Figure 5: AODV RREP transition diagram

4.3 Detection of attacks

In this section, we describe how our proposed intrusion detection system can detect attacks against the AODV protocol. These attacks are described in table 1 in section 2.2.

False message propagation of RREQs (attack 1): First, the AODV specification determines if the transmitted route request originates from the node, i.e., the originator IP address of the RREQ is equal to the IP address of the node. In this case, the answer is no. Thus, the specification assumes that the route request originates from another node and start searching for the corresponding route request among the received route request messages. However, the corresponding route request message is not found, since the RREQ message is false. Thus, the AODV state machine reaches the *invalid RREQ* state.

False message propagation of RREPs (attack 2): The transmitted RREP is not among the received route replies messages (RREP forward state). Neither is the RREP a route reply to a received RREQ (RREP originated by the node state). Thus, the AODV state machine enters the *invalid RREP* state.

False route reply and modify routing table (attack 3 and 9): The transmitted RREP is either a *RREP by intermediate node* or a *RREP by the destination*. If the RREP is performed by an intermediate node and the node has a route to the destination in its routing table with the specified sequence number and hop count, the RREP is valid. Otherwise, the RREP is an attack and thus the state machine reaches the *invalid RREP* state. If the RREP is performed by the destination, the RREP is valid if the hop count value is zero and the sequence number is the current sequence number of the node. However, an adversary can also modify the routing table. Thus, the IDS agent must maintain its own routing table and thus also detect if the routing table is modified.

Rushing (attack 4): In a rushing attack, a malicious node sends RREQ messages with a false originator IP address. Thus, this attack is detected in a similar way as attack 1. That is, the RREQ is neither present among the received route request messages (RREQ forward state) nor is the originator IP address of the RREQ equal to the IP address of the node (RREQ initiate state). Thus, the AODV state machine enters the *invalid RREQ* state.

Modification of routing messages (attack 5): The IDS agent gathers received route request messages and route reply messages in order to be able to detect if any field of the transmitted routing messages has been modified.

Resource depletion attack (attack 6): The AODV protocol specifies that the node should not originate more than RREQ_RATELIMIT RREQ messages per second. Thus, the node is considered to perform a flooding attack if this rule is broken. However, the node could also flood the network by using a false IP address. The detection of false RREQs and false RREPs are described above, see attack 1 and attack 2.

Dropping of routing packets (attack 7): The IDS agent gathers received route request and route reply messages. When the IDS agent detects a valid routing message that is transmitted and also corresponds to a certain received routing message that message is drooped from the list of received packets. Periodically, the IDS agent verifies if any received routing message is older than a certain value. If so, the IDS agent assumes that the node has neglected to forward the routing message. Thus, the node has dropped the routing packet.

Routing table overflow (attack 8): Routing table overflow is performed by sending false RREQs or RREPs with non-existing addresses, see attack 1 and attack 2 above.

6.0 CONCLUSION

We have argued that intrusion detection must be included in the security architecture for mobile ad hoc networks to achieve adequate security. This is especially true for tactical mobile ad hoc networks deployed in hostile environments, since these networks include vulnerabilities that an adversary can exploit. However, the current intrusion detection techniques developed for civilian wireless networks can not be applied to mobile ad hoc networks. Thus, a new architecture is needed. Moreover, new techniques are needed to detect attacks against protocols developed for mobile ad hoc networks.

To suit the architecture of mobile ad hoc networks, intrusion detection should be performed without cooperative participation with other nodes. We propose an architecture, based on specification-based detection, which detects intrusions within the node. Thus, the intrusion detection system will determine if the node itself is misbehaving and also internally respond to detected intrusions. The advantage with internally performed responses is that an adversary can not produce malicious responses against other nodes. Nevertheless, the methods of internally performed response are just as effective as global response (proposed by other researchers [2]) and also easier to perform. Another advantage is that detection of attacks and response against these attacks are performed without collaboration with other nodes. It is not a trusted method to detect attacks from other nodes by cooperating with these nodes, since one of these nodes may be a malicious node.

The aim of the intrusion detection system is to detect if someone with or without physically access have infiltrated the system and performs attacks against other nodes. Thus, the intrusion detection system must considerably delay unauthorized access to prevent that an adversary also modifies the intrusion detection system. To accomplish this, the intrusion detection system is put in the network card in a tamper-resistant processor with its own memory. This will hinder an adversary without physically access to modify the intrusion detection system. The tamper-resistant processor will probably also hinder, or at least

considerably delay, an adversary from modifying the intrusion detection system. A considerable delay is enough, since an adversary with physically access only can use the system for malicious purposes during a limited time due to the fact that the keys are exchanged regularly.

Finally, we have also presented a specification-based approach that detects attacks based on a set of constraints that describes the correct operations of the protocols. We have shown, by examples, that the approach can detect attacks (with serious consequences) against the routing protocol AODV. It has been proved for wired networks that specification-based methods provide a low false positive rate, i.e. few false alarms, and can detect previously unknown attacks. Currently, we are continuing our investigation by proving that our proposal also provides a low false positive rate and a high detection rate. Furthermore, the AODV specification will be extended with a model for route error messages in order to detect route error attacks.

REFERENCES

[1] H. Debar, B. Morin. “Intrusion detection – Evaluation of the diagnostic capabilities of commercial intrusion detection systems.” Proceedings of RAID. Lecture Notes in Computer Science. Vol. 2516. Pages: 177-198. 2002.

[2] Y. Zhang, W. Lee and Y. Huang. “Intrusion Detection Techniques for Mobile Wireless Networks. In Report on a Working Session on Security in Wireless Ad Hoc Networks”. *Mobile Computing and Communications Review*. Vol. 7, No. 1. Pages: 74-94. ACM. January, 2003.

[3] Y. Hu, A. Perrig, et al., “Ariadne: A secure on-demand routing protocol for ad hoc networks”, *MobiCom 2002*, September 2002

[4] L. Zhou, Z. Haas, “Securing Ad Hoc Networks”, *IEEE Network Magazine*, Nov/Dec 1999

[5] Y. Zhang, W. Lee. “Intrusion Detection in Wireless Ad hoc Networks”. *Proceedings of MOBICOM*. Pages: 275-283. ACM. 2000.

[6] C. Ko, M. Ruschitzka, and K. Levitt, “Execution Monitoring of Security Critical Programs in Distributed Systems: A Specification-based approach, “ *In Proceedings of Symposium on Security and Privacy*, 1997.

[7] C. Ko, P. Brutch, J. Rowe, Tasfnat and K. Levitt, “System Health and Intrusion Monitoring using a Hierarchy of Constraints”, *In Proceedings of 4th International Symposium on Recent Advances in Intrusion Detection*, 2001.

[8] A. Mishra, K. Nadkarni, A. Patcha. ”Intrusion Detection in Wireless Ad Hoc Networks”. *Wireless Communications*. Pages: 48-60. IEEE. February, 2004.

[9] V. Gupta; “Denial of service attacks at the MAC layer in wireless ad hoc networks”, proc. *Milcom 2002*, October 2002.

[10] S. Wong, “The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards”, May 20, 2003.

[11] N. Moore, “Optimistic Duplicate Address Detection for IPv6”, draft-ietf-ipv6-optimistic-dad-02.txt, September 2004

[12] S. Thomson et al., “IPv6 Stateless Address Autoconfiguration”, RFC 2462, December 1998.

[13] C. Perkins et al., “Ad hoc On-Demand Distance Vector (AODV) Routing”, RFC 3561, July 2003.

[14] S. Axelsson, “Intrusion Detection Systems: A Taxonomy and Survey, ”Tech. Report no. 99-15, Dept. of Comp. Eng., Chalmers Univ. of Technology, Sweden, Mar. 20, 2003

[15] S. Marti et al., “Mitigating Routing Misbehaviour in Mobile Ad Hoc networks”, *Proc. 6th Annual Int’l. Conf. Mobile Comp. and Net.*, Boston, MA, pp. 255-65.

[16] I. Chisalita et al, “Suitability of Wireless Intrusion Detection Tools in Tactical Mobile Ad hoc Networks, Oct. 2004.

[17] National institute of standards and technology, *Finite state machine*, http://www.nist.gov/dads/HTML/finiteStateMachine.html (accessed 050206)

[18] Finite state machines, http://spinroot.com/spin/Doc/Book91_PDF/ch8.pdf (accesses 050206)

[19] V. Goyal. “How to re-initialize a hash chain”, http://eprint.iacr.org/ 2004/097.pdf (accesses 050310)